Guardian Digital
Internet Defense and Detection System

IDDS Guide

Copyright ©2000 - 2003 Guardian Digital, Inc.

Contents

1 INTRODUCTION **1**

2 CONTACTING GUARDIAN DIGITAL **2**

3 TECHNICAL SUPPORT **3**

4 Internet Defense and Detection System **5**

4.1 Installing IDDS 5

4.2 Configuring IDDS 5
4.2.1 General Operation 6
4.2.2 Rule Configuration 10
4.3 Graphs and Reports 11
4.3.1 Active Reports 11
4.3.2 IDDS Report Archives 14
4.4 Real-Time Attack Listing 15
4.5 Export Attack Data 16

1 INTRODUCTION

Welcome to the Guardian Digital Internet Acceleration and Management Server! This QuickStart Guide provides information about the IAM Server and describes the steps necessary to successfully install and configure it.

For more detailed information about how to use EnGarde Secure Professional, be sure to refer to the complete EnGarde Secure Professional Users Guide.

2 CONTACTING GUARDIAN DIGITAL

Guardian Digital welcomes your input and feedback. You may direct all questions, commands, or requests concerning the software you purchased, your registration status, or similar issues to the Guardian Digital Customer Service department at the following address:

Guardian Digital Customer Service
165 Chestnut Street
Allendale, New Jersey 07401
United States

Phone:	+1-201-934-9230
E-Mail:	customer.service@guardiandigital.com
World Wide Web:	http://www.guardiandigital.com
Online Store:	http://store.guardiandigital.com

The department's hours of operation are 9:00 AM to 7:00 PM Eastern Time, Monday through Friday.

3 TECHNICAL SUPPORT

Guardian Digital provides comprehensive support for your enterprise. Guardian Digital can help bridge the gap between the fast-paced nature of the Internet, security, and the latest open source technologies available in EnGarde. Guardian Digital can provide you with the information necessary to develop unique customizations of EnGarde products to achieve the fastest time to market with the most cost-effective solutions.

Included with your purchase is 60 days of e-mail, telephone, and Web installation and configuration support beginning at the time of purchase. This includes up to four incidents of installation and configuration support within that 60 day period.

Guardian Digital encourages you to visit us on the Web for the answers to many commonly asked questions and system documentation. Contact Guardian Digital Technical Support between the hours of 9:00 AM and 7:00 PM Eastern time.

To provide the answers you need quickly and efficiently, the Guardian Digital Technical Support staff needs some information about your computer and software. Please include this information in your correspondence:

- Program name and version number
- Product registration number
- Any additional hardware or peripherals connected to your computer
- How to reproduce your problem: when it occurs, whether you can reproduce it regularly, and under what conditions

- Information needed to contact you by voice, fax, or e-mail
- Steps you have taken thus far to try to resolve the problem
- Any additional software installed

Please contact us using one of the following methods:

Phone:	+1-201-934-9230
E-Mail:	support@guardiandigital.com
World Wide Web:	http://www.guardiandigital.com

To avoid delay in processing your request, be sure to include your account number in the subject of the e-mail.

4 Internet Defense and Detection System

The Guardian Digital Internet Defense and Detection System (IDDS) will track incoming and outgoing traffic on your network. Using a pre-defined set of rules the IDDS will determine if the traffic is malicious. The IDDS will search for attacks against servers and services such as Denial of Service (DoS) attacks, it will also track the use of an array of protocols which may be against company policy and track possible misuse of the network.

Additionally IDDS keeps detailed reports and graphs in real-time and over time. The IDDS will also archive all reports for a given day, week or month.

4.1 Installing IDDS

The Guardian Digital Internet Defense and Detection System is installed via the Guardian Digital Secure Network (GDSN). To install the IDDS insert the CD-ROM disk that was included with the Guardian Digital IDDS purchase into the CD-ROM drive of the EnGarde server you will be installing the IDDS on.

Selecting *Install from Local Media* in the GDSN will perform the installation. Instructions on how to use the GDSN can be found in *Section 5* on page *171* of EnGarde Secure Professional User Manual. Additionally the *Install from Local Media* portion can be located on page *173* under *Section 5.1.2 Install from Local Media*.

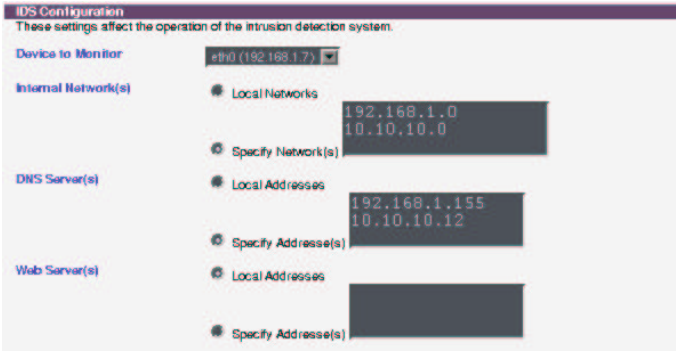
4.2 Configuring IDDS

After installation you can find the IDDS modules in the *Security* section of the WebTool main menu.

To configure the *Intrusion Detection System* on your EnGarde server select the *IDDS Management* option from the *Security* menu. Select *Edit Configuration* to begin configuring the IDDS.

4.2.1 General Operation

Configuring the IDDS is a relatively painless task. Leaving all the configuration options set to their default settings will allow the IDDS to scan the local internal network(s) that the IDDS is located on. To limit the IDDS to monitor specific subnets on the internal network they must be specified separately by selecting the *Specify Network(s)* option and then entering in the network(s). A description of what each option is and how to use it is below.



Device To Monitor To be effective, the IDDS needs to be told which interface it should monitor for malicious activity. If your machine has only one interface, select it from the drop down. If your machine has multiple interfaces, select the "external" one. If you are unsure, select eth0.

Internal Network(s) This is a listing of networks which are deemed "local" to the IDDS subsystem. These networks will be used when matching "destination addresses" in the attack patterns.

You may enter one network of the form `1.2.3.4/5` where '`1.2.3.4`' is a network address and '`5`' is the netmask in CIDR notation. For a definition of CIDR see the end of this section on page *7*.

To add multiple addresses, specify one per line.

DNS Server(s) This is a listing of the IP addresses of machines you use as DNS servers. This will help limit the number of false positives on DNS-related attacks.

Multiple entries are handled like above.

Web Server(s) This is a listing of the IP addresses of machines you use as web servers. This will help limit the number of false positives on WWW-related attacks.

Multiple entries are handled like above.

What is CIDR Notation

Classless Inter Domain Routing (CIDR) is a method for assigning IP addresses without using the standard IP address classes like Class A, Class B or Class C.

In CIDR notation, an IP address is represented as A.B.C.D /n, where "/n" is called the IP prefix or network prefix. The IP prefix identifies the number of significant bits used to identify a network. For example, 192.9.205.22 /18 means, the first 18 bits are used to represent the network and the remaining 14 bits are used to identify hosts. Common prefixes are 8, 16, 24, and 32.

Refer to the following page for the *CIDR to Netmask Translation Table*.

CIDR	Netmask (Dot Notation)	Number of Hosts
/1	128.0.0.0	
/2	192.0.0.0	
/3	224.0.0.0	
/4	240.0.0.0	
/5	248.0.0.0	
/6	252.0.0.0	
/7	254.0.0.0	
/8	255.0.0.0	
/9	255.128.0.0	
/10	255.192.0.0	
/11	255.224.0.0	
/12	255.240.0.0	
/13	255.248.0.0	
/14	255.252.0.0	
/15	255.254.0.0	
/16	255.255.0.0	
/17	255.255.128	
/18	255.255.192.0	
/19	255.255.224.0	
/20	255.255.240.0	
/21	255.255.248.0	
/22	255.255.252.0	
/23	255.255.254.0	
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32
/28	255.255.255.240	16
/29	255.255.255.248	8
/30	255.255.255.252	4
/31	255.255.255.254	2
/32	255.255.255.255	1

4.2.2 Rule Configuration

The Intrusion Detection System works on a set of given rules. How it makes use of these rules is by checking the data it sees on the network against these rules. If a piece of data matches a set rule it then takes action according to the rule. The rule defines the type of traffic, the priority of the traffic, and sort it into a proper class.

The IDDS then keeps track of all data in detailed logs. These logs are used to create detailed graphs and reports that are generated on a daily, weekly and monthly basis. More information concerning these reports can be found in *Section 4.3* on page *11*.

To enable a rule check its associated box and vice-versa to disable a rule. To get an explanation of each rule click on the rule itself. A smaller window will appear with a description of the rule and what it does.

When changes have been completed click the *Save Changes* button.

The IDDS system is now ready to be started. By clicking the *Start IDDS* option, located at the bottom of the *IDDS Management* page will start the IDDS. The screen will refresh and there will now be a second option to stop the IDDS. The Intrusion Detection System is now running.

4.3 Graphs and Reports

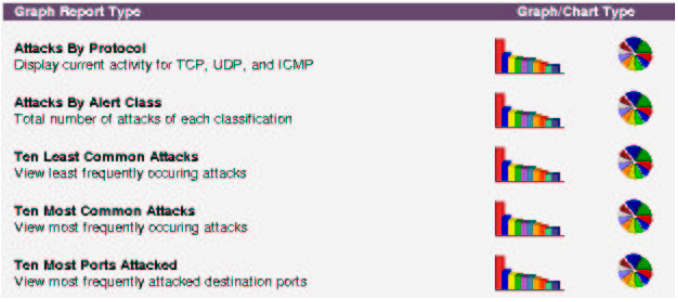
The Intrusion Detection System logs all the data it collects from the network. That data is then used to compile numerous graphs and charts. These graphs and charts are created daily, weekly and monthly and are archived accordingly. Additionally, there are real-time graphs that display live information for your network.

To access the Graphs and Reports select the *Graphs and Reports* option from the *IDDS Management* screen.

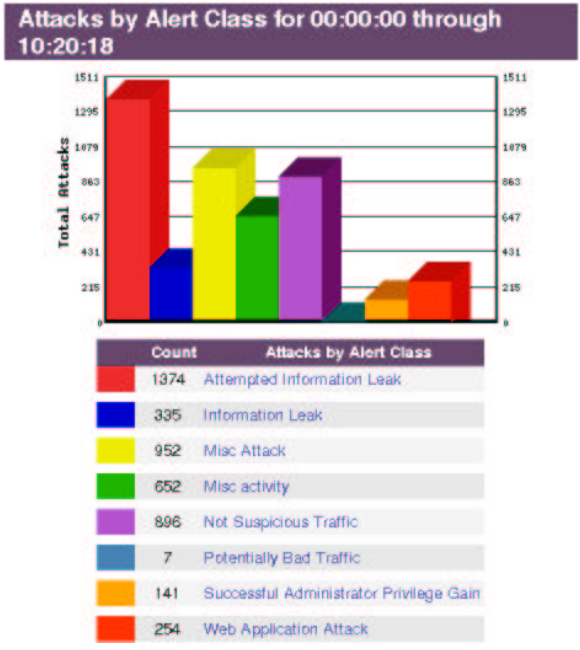
The *Graphs and Reports* section is broken down into two smaller sections. There are the *Active Reports* and the *Report Archives.*

4.3.1 Active Reports

The Active Reports section allows you to choose a report type and how you would like the graph contained within the report displayed, as a pie chart or bar graph. You can view the report by clicking in the icon of a pie chart or a bar graph and the associated report will be displayed.

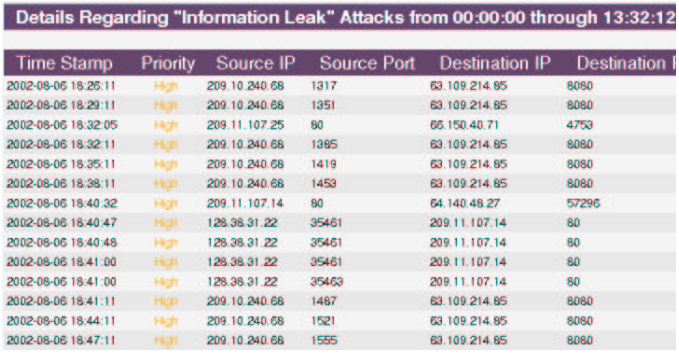

Graph Report Type
Graph/Chart Type
Attacks By Protocol
Display current activity for TCP, UDP, and ICMP
Attacks By Alert Class
Total number of attacks of each classification
Ten Least Common Attacks
View least frequently occuring attacks
Ten Most Common Attacks
View most frequently occuring attacks
Ten Most Ports Attacked
View most frequently attacked destination ports

The report may take a few moments to be displayed since these numbers are gathered and the reported being generated when you click on the icon.



Once the report is displayed you will see the report type along with the time period the report covers followed by the graph and a breakdown of each item in the graph. Each highlighted item in the graph can be clicked on to view details concerning that item.

For example, if *Attacks by Alert Class* was chosen, a graph displaying the different protocols will be displayed. In the example above, if *Information Leak* was chosen, all the source hosts attempting this exploit in to the Information Leak alert class will be displayed in detail.



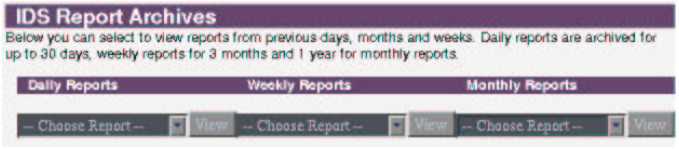
Details Regarding "Information Leak" Attacks from 00:00:00 through 13:32:12

Time Stamp	Priority	Source IP	Source Port	Destination IP	Destination I
2002-08-06 18:26:11	High	209.10.240.68	1317	63.109.214.85	8080
2002-08-06 18:29:11	High	209.10.240.68	1351	63.109.214.85	8080
2002-08-06 18:32:05	High	209.11.107.25	80	66.150.40.71	4759
2002-08-06 18:32:11	High	209.10.240.68	1385	63.109.214.85	8080
2002-08-06 18:35:11	High	209.10.240.68	1419	63.109.214.85	8080
2002-08-06 18:38:11	High	209.10.240.68	1453	63.109.214.85	8080
2002-08-06 18:40:32	High	209.11.107.14	80	64.140.48.27	57296
2002-08-06 18:40:47	High	128.38.31.22	35461	209.11.107.14	80
2002-08-06 18:40:48	High	128.38.31.22	35461	209.11.107.14	80
2002-08-06 18:41:00	High	128.38.31.22	35461	209.11.107.14	80
2002-08-06 18:41:00	High	128.38.31.22	35463	209.11.107.14	80
2002-08-06 18:41:11	High	209.10.240.68	1487	63.109.214.85	8080
2002-08-06 18:44:11	High	209.10.240.68	1521	63.109.214.85	8080
2002-08-06 18:47:11	High	209.10.240.68	1555	63.109.214.85	8080

This works for all the graphs in this section.

4.3.2 IDDS Report Archives

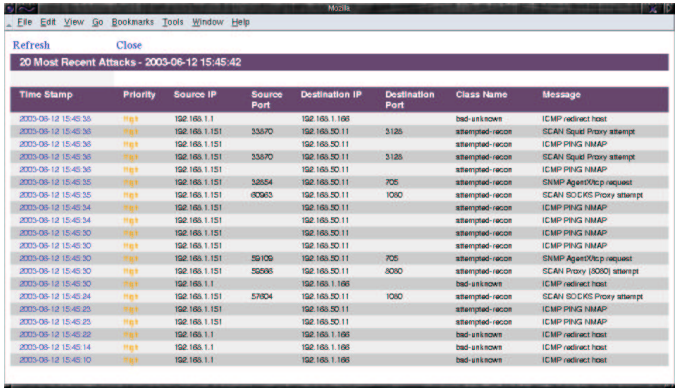
The Intrusion Detection System uses its logs to produce reports. All the reports created are stored on the server for future reference. Daily, weekly and yearly reports are created and stored. Daily reports are created at midnight for the previous day and are kept for 30 days before the system removes them. Weekly reports are for the previous week (7 days) and removed after 3 months (90 days) and monthly reports are for the prior month (30 days) and are removed after one year.


IDS Report Archives
Below you can select to view reports from previous days, months and weeks. Daily reports are archived for up to 30 days, weekly reports for 3 months and 1 year for monthly reports.
Daily Reports
Weekly Reports
Monthly Reports
-- Choose Report --
View
-- Choose Report --
View
-- Choose Report --
View

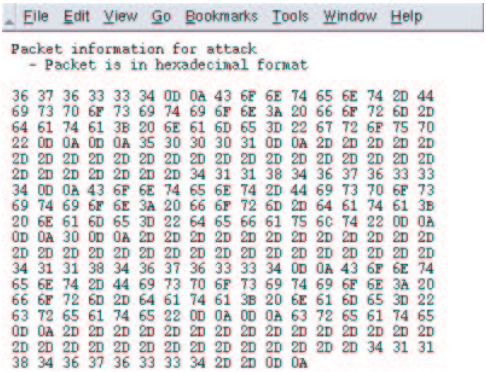
To access a report, select from the daily, weekly or monthly pull-down menu.

4.4 Real-Time Attack Listing

The *Real-Time Attack Listing* will open a new window that will display the 20 most recent attacks in 5 second increments.


Mozilla
File Edit View Go Bookmarks Tools Window Help
Refresh
Close
20 Most Recent Attacks - 2003-06-12 15:45:42
Time Stamp
Priority
Source IP
Source Port
Destination IP
Destination Port
Class Name
Message
2003-06-12 15:45:36 high 192.168.1.1 192.168.1.166 bad-unknown ICMP redirect host
2003-06-12 15:45:36 high 192.168.1.151 33870 192.168.50.11 3128 attempted-recon SCAN Squid Proxy attempt
2003-06-12 15:45:36 high 192.168.1.151 192.168.50.11 attempted-recon ICMP PING NMAP
2003-06-12 15:45:36 high 192.168.1.151 33870 192.168.50.11 3128 attempted-recon SCAN Squid Proxy attempt
2003-06-12 15:45:36 high 192.168.1.151 192.168.50.11 attempted-recon ICMP PING NMAP
2003-06-12 15:45:35 high 192.168.1.151 32854 192.168.50.11 705 attempted-recon SNMP AgentX/tcp request
2003-06-12 15:45:35 high 192.168.1.151 60965 192.168.50.11 1080 attempted-recon SCAN SOCKS Proxy attempt
2003-06-12 15:45:34 high 192.168.1.151 192.168.50.11 attempted-recon ICMP PING NMAP
2003-06-12 15:45:34 high 192.168.1.151 192.168.50.11 attempted-recon ICMP PING NMAP
2003-06-12 15:45:30 high 192.168.1.151 192.168.50.11 attempted-recon ICMP PING NMAP
2003-06-12 15:45:30 high 192.168.1.151 192.168.50.11 attempted-recon ICMP PING NMAP
2003-06-12 15:45:30 high 192.168.1.151 59109 192.168.50.11 705 attempted-recon SNMP AgentX/tcp request
2003-06-12 15:45:30 high 192.168.1.151 52586 192.168.50.11 8080 attempted-recon SCAN Proxy (8080) attempt
2003-06-12 15:45:30 high 192.168.1.1 192.168.1.166 bad-unknown ICMP redirect host
2003-06-12 15:45:24 high 192.168.1.151 57604 192.168.50.11 1080 attempted-recon SCAN SOCKS Proxy attempt
2003-06-12 15:45:23 high 192.168.1.151 192.168.50.11 attempted-recon ICMP PING NMAP
2003-06-12 15:45:23 high 192.168.1.151 192.168.50.11 attempted-recon ICMP PING NMAP
2003-06-12 15:45:22 high 192.168.1.1 192.168.1.166 bad-unknown ICMP redirect host
2003-06-12 15:45:14 high 192.168.1.1 192.168.1.166 bad-unknown ICMP redirect host
2003-06-12 15:45:10 high 192.168.1.1 192.168.1.166 bad-unknown ICMP redirect host

The attacks will be sorted by time. By clicking on the time stamp of the attack the packet information for that attack will be displayed.



4.5 Export Attack Data

Aside from the creation of the daily, weekly and monthly reports the IDDS system will create CSV files of this data as well.

Predefined Time Specifications

The IDDS system will generate CSV files for the previous day, week and month that will be available for immediete download.

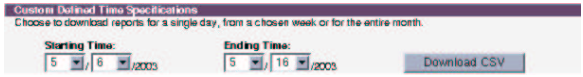
Predefined Time Specifications
Choose to download reports for a single day, from a chosen week or for the entire month.
Daily CSV
-- Choose Day --
Download CSV
Weekly CSV
-- Choose Week --
Download CSV
Monthly CSV
-- Choose Month --
Download CSV

There are pull-down menus for daily, weekly and monthly. Select the CSV to download and click the corrisponding *Download CSV* button to retrieve the CSV for the specified time period.

NOTE: All CSVs are compressed due to their large size.

Custom Defined Time Specifications

In addition to the predefiined time periods to download in CSV there is also the *Custom Defined Time Specifications* sections. This will allow a CSV of the specified time period to be generated and downloaded.


Custom Defined Time Specifications
Choose to download reports for a single day, from a chosen week or for the entire month.
Starting Time:
5 / 6 /2003
Ending Time:
5 / 16 /2003
Download CSV

To make a date selection choose a month from the first pull-down menu and a day from the second pull-down. Do the same for the ending date and then click the Download CSV button. Unlike the *Predefined Time Specifications* since the data is gathered and the CSV generated at the time the dates are selected. On slower machines with a good deal of data this can be time consuming.

Once the report has been generated you will be prompted to save the CSV file. As with the *Predefined Time Specifications* CSVs, these are compressed.